Business Wire
The Global Leader in News Distribution

Riptech Further Expands Management Team Amid Strong Demand for Real- Time Managed Security Services

Business Wire; New York; Jul 25, 2001; Business Editors/Hi-Tech Writers;

*Sic:*541611*Sic:*7379
Start Page: 1
Companies: Hunter Group*Sic:*541611*Sic:*7379
Riptech Inc

Abstract:

Riptech, Inc., the premier provider of scalable, real-time managed security services, protects clients through advanced outsourced security monitoring and professional services. Riptech's unique Caltarian technology platform provides real-time information protection through around-the-clock monitoring, analysis, and response. The Caltarian technology is capable of processing large volumes of network security data to separate security threats from false positives in real-time, with carrier-class scalability. Additionally, Riptech's Security Professional Services group provides security policy development, assessment and auditing, penetration testing, incident forensics, and response. Riptech security specialists have secured hundreds of organizations including Fortune 500 companies and federal agencies. Founded in 1998 by former Department of Defense security professionals and market experts, Riptech is headquartered in Alexandria, Virginia with offices in San Jose, California, and New York City.

Riptech, the Riptech logo, Caltarian, and Real-Time Information Protection are trademarks or service marks of Riptech, Inc. Other products mentioned herein may be trademarks and/or registered trademarks of their respective owners.

Full Text:
Copyright Business Wire Jul 25, 2001

ALEXANDRIA, Va.--(BUSINESS WIRE)--July 25, 2001--

FutureNext Consulting Co-founder and The Hunter Group Executive Vice President Loren Burnett Appointed Senior Vice President and Chief Financial Officer; Elad Yoran Assumes Executive Vice President for Corporate Development and Chief Marketing Officer Responsibilities

Riptech(sm), Inc., the premier provider of scalable, real-time managed security services, today announced the further expansion of its management team to support rapid corporate growth amid increasing demand for its real-time managed security services. Loren Burnett, a financial management veteran, has been named senior vice president and chief financial officer. Riptech CFO Elad Yoran has been named executive vice president for corporate development and chief marketing officer. The announcement strengthens the management team while emphasizing Riptech's commitment to partners and customers.

"Elad Yoran and Loren Burnett bring tremendous combined experience and leadership to Riptech as we execute our strategy for rapid growth," said Amit Yoran, president and CEO of Riptech, Inc. "Their strong management skills will be crucial to Riptech's success as we continue to provide unparalleled managed security services for our clients and partners."

"I am pleased to join Riptech's dynamic and extremely capable team," said Loren Burnett, CFO of Riptech, Inc. "I look forward to executing the next phase of our rapid and disciplined growth strategy as we capitalize on our position of strength in the managed security services market."

Prior to joining Riptech, Mr. Burnett served as co-founder, CFO, and COO of FutureNext Consulting, where he directed the company's $75 million equity fundraising efforts and services delivery organization. Additionally, Mr. Burnett also served as CFO, senior vice president of finance and administration, and a member of the board of The Hunter Group, an $80 million global provider of management consulting services. Mr. Burnett managed the filing of The Hunter Group's IPO and subsequent $155 million sale to Renaissance Solutions.

A 22-year industry veteran, Mr. Burnett served as the CFO of Maxm Systems and has held financial management positions at National Telephone Services and MCI Communications. Mr. Burnett also served with the accounting firm Coopers & Lybrand. A graduate of the University of Delaware, Mr. Burnett is a Certified Public Accountant in the Commonwealth of Virginia and a member of the American Institute of Certified Public Accountants.

"Riptech's scalable Caltarian technology platform, combined with our extensive sales channel and the excellence of our monitoring and management services, has given us a strong lead in the managed security services market," said Elad Yoran, executive vice president for corporate development and CMO of Riptech, Inc. "By expanding our marketing and corporate development strategy, we will capitalize on this lead as we continue to grow."

Prior to co-founding Riptech, Mr. Yoran was a vice president with Broadview International, an investment bank that specializes in mergers and acquisitions for information technology and media companies. While at Broadview, Mr. Yoran was responsible for analyzing and evaluating information security technologies, companies, and market dynamics. Through his role in identifying and executing merger and acquisition opportunities for both public and private companies, Mr. Yoran was a driving force in the security market's consolidation.

Mr. Yoran served as an officer in the U.S. Army, where he managed the deployment of Global Positioning Systems field applications. He is a combat veteran of Operation Restore Hope in Somalia. Mr. Yoran is an MBA graduate of the Wharton School of the University of Pennsylvania and holds a BS degree in Mechanical Systems Engineering Management with honors from the United States Military Academy at West Point.

About Riptech

Riptech, Inc., the premier provider of scalable, real-time managed security services, protects clients through advanced outsourced security monitoring and professional services. Riptech's unique Caltarian technology platform provides real-time information protection through around-the-clock monitoring, analysis, and response. The Caltarian technology is capable of processing large volumes of network security data to separate security threats from false positives in real-time, with carrier-class scalability. Additionally, Riptech's Security Professional Services group provides security policy development, assessment and auditing, penetration testing, incident forensics, and response. Riptech security specialists have secured hundreds of organizations including Fortune 500 companies and federal agencies. Founded in 1998 by former Department of Defense security professionals and market experts, Riptech is headquartered in Alexandria, Virginia with offices in San Jose, California, and New York City.

Riptech, the Riptech logo, Caltarian, and Real-Time Information Protection are trademarks or service marks of Riptech, Inc. Other products mentioned herein may be trademarks and/or registered trademarks of their respective owners.

RealSecure

Computer Reseller News; Manhasset; Oct 27, 1997; Anonymous;

Issue:	760
Start Page:	182
ISSN:	08938377
Subject Terms:	Software reviews
	Internet
	Computer security
Classification Codes:	**9120**: *Product specific treatment*
	5240: *Software & systems*
	5140: *Security management*
	9190: *US*
Geographic Names:	US
Companies:	**Internet Security Systems Inc**

Abstract:

Internet Security Systems Inc.'s RealSecure is reviewed. The product monitors network traffic without affecting performance, analyzes packets for unauthorized activity and known attack patterns, and identifies intruders. If an intrusion is detected, RealSecure alerts personnel via e-mail or pager, logs the event and pertinent data, and kills the attack by terminating its connection before damage is done. RealSecure guards against unauthorized attempts to get at password files, remote registry access attempts, null session attempts, and attempts to read and write from protected directories.

Full Text:

Price: $4,995 Warranty: 90 days

Distributors/Integrators: Distributes to systems integrators and VARs Authorization Requirements: $5,000 entry fee, maintain at least one ISS certified engineer on staff, annual license volume of $250,000

Model Number: RS-1-P

Internet Security Systems Inc. Atlanta, Ga. (770) 395-0150 www.iss.net

FIREWALLS ARE IMPERFECT security devices. Notoriously hard to configure, a savvy hacker can easily break through. RealSecure guards against intruders and reveals network weak spots. This product monitors network traffic without affecting performance, analyzes packets for unauthorized activity and known attack patterns, and identifies intruders.

If an intrusion is detected, RealSecure alerts personnel via Email or pager, logs the event and pertinent data, and kills the attack by terminating its connection before damage is done. RealSecure guards against unauthorized attempts to get at password files, remote registry access attempts, null session attempts, and attempts to read and write from protected directories.

RealSecure is more effective than having a person monitoring network activity for foul play because RealSecure can detect intrusions lasting only a few milliseconds. If attacks do get through a firewall-or come from behind the firewall-RealSecure logs the activity in an,ODBC-compliant database. This way, a network administrator can figure out where the attack originated and how to prevent future attacks through the same security breach.

RealSecure can be deployed across an entire enterprise network with engines placed on critical network segments, all reporting to a centralized management console.

RealSecure was the easiest Internet security application to install of all those tested but did require a fairly high knowledge base of the site infrastructure. RealSecure's simple point-and-click interface is top-notch. Documentation is good, though rarely needed.

RealSecure more than meets its primary goal of monitoring for attacks, although it really is just a partial solution. RealSecure is not nearly as important as a basic firewall, nor can it substitute for one. RealSecure is more of a stand-alone product and does not integrate with all security products, but it does support multiple sites and servers.
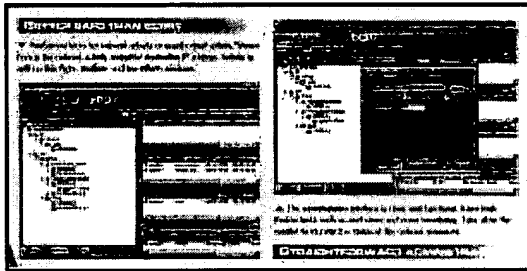
Net monitoring tools gain real-time alerts

Computerworld; Framingham; Apr 14, 1997; Sharon Machlis;

Volume:	31
Issue:	15
Start Page:	16
ISSN:	00104841
Subject Terms:	Product development
	Software packages
	Computer security
	Computer networks
	Hackers
	Product introduction
	Network management systems
	Software
	Computer security
	Real time
Classification Codes:	9190: *US*
	7500: *Product planning & development*
	5240: *Software & systems*
	5140: *Security management*
Geographic Names:	US
Companies:	**Internet Security Systems Inc**
	Intrusion Detection Inc
	Internet Security Systems Inc
	Intrusion Detection Inc

Abstract:
Internet Security Systems of Atlanta will soon begin beta-testing a Windows NT version of its RealSecure monitoring package, following a Unix version released in December 1996. Intrusion Detection Inc. in March 1997 announced the Kane Security Monitor for Windows NT that will look for things such as multiple log-on tries or attempts to access a top executive's PC. The products join a class of tools that guards against insider snooping and mischievous outsiders. If suspicious activity is discovered, the system often takes defensive measures and notifies a security administrator by E-mail or pager. Many monitors look for the signatures of well-known hacker attack patterns and advise users of new rules as the art of hacking advances.

Full Text:
Copyright CW Communications/Inc. Apr 14, 1997

ANALYZING LOGS after a break-in won't protect your computer network any more than reviewing surveillance camera footage from time to time would adequately safeguard a bank.

So security firms are moving to the next generation of network monitoring tools: realtime detection and reaction.

"I think it's great that we're seeing more intelligence in these products," said Gary Lynch, a vice president for business continuation and data security at Prudential Insurance Company of America in Roseland, N.J. "Having no tools or 'historical' tools won't cut it anymore."

ON TAP

Internet Security Systems of Atlanta next month will begin beta-testing a Windows NT version of its RealSecure monitoring package, following a Unix version released in December. And Intrusion Detection, Inc. in New York last month announced the Kane Security Monitor for Windows NT that will look for things such as multiple log-on tries or attempts to access a top executive's PC.

The products join recently introduced offerings such as NetRanger from WheelGroup Corp. in San Antonio; WebStalker-Pro for Windows NT from Haystack Labs, Inc. in Austin, Texas; and OmniGuard/Intruder Alert from Axent Technologies, Inc. in Rockville, Md.

That class of tools guards against insider snooping and mischievous outsiders.

If suspicious activity is discovered, the system often takes defensive measures - for example, blocking electronic-mail floods or shutting off a connection trying to tap in to a password file - and notifies a security administrator by E-mail or pager.

Depending on the product, a monitor can sit at a firewall connection, on servers or on individual desktop computers. Somewhat like antivirus software, many monitors look for the signatures of well-known hacker attack patterns and advise users of new rules as the art of hacking advances.

"Its purpose and what the product does is great," said Roger Caissie, security analyst for information systems security at Toronto Dominion Bank, an early user of Axent software. But Caissie said he doesn't use it as much as he would like because his department hasn't found the time to set up all the rules and responses. He said he expects that a future version will have default settings to make it easier and faster to configure.

The ultimate idea is to save time and money, and to boost safety -- although experts say the software augments welltrained security personnel and doesn't replace them.

Having a $5,ooo software package do preliminary monitoring work makes more sense than using a $100,000-a-year security specialist, Lynch said. "I'd rather pay a person to do the follow-through," he said.

Most users are hesitant to discuss which monitoring tools they've implemented and how they work for fear of inadvertently issuing a challenge to hackers.

Without specifying the software used or the attack it stopped, Lynch said that "in one case, it did what it was designed to do. We are certainly making use of these tools."

REAL-TIME NETWORK MONITORING
TOOLS

Managed security services are gaining new players

Network World; Framingham; Apr 2, 2001; Ellen Messmer;

Volume:	18
Issue:	14
Start Page:	14
ISSN:	08877661
Subject Terms:	Computer security
	Systems management
	Outsourcing
	Service introduction
Classification Codes:	**9190**: *United States*
	8302: *Software & computer services industry*
	5140: *Security management*
Geographic Names:	United States
	US

Abstract:

Managed security services are catching on because they offer corporations a way to hire outside experts to remotely manage firewalls, VPNs and intrusion-detection equipment. Securify has built monitoring equipment that can process intranet traffic on LAN segments at 100M bit/sec to report back network-based events that depart from accepted business use. By consulting with a company to understand how employees and business partners allowed inside the intranet use the network on a daily basis, Securify determines the security policy for appropriate use. Another security firm, RipTech, introduced its managed security service, dubbed Caltarian RipTech installs and remotely monitors any of six types of firewalls, intrusion-detection systems and VPNs from its Alexandria, Va., data center.

Full Text:

[Headnote]

Two security companies and Cisco have separate offerings in the works.

Managed security services are catching on because they offer corporations a way to hire outside experts to remotely manage firewalls, VPNs and intrusion-detection equipment.

This week, two security firms - plus giant Cisco - are each stepping into this arena with their own approaches.

Securify was founded three years ago by Taher Elgamal, inventor of the Web's encryption technology Secure Sockets Layer. It was a consultancy but is now jumping into the managed security services arena. Securify has built monitoring equipment that can process intranet traffic on LAN segments at I OOM bit/sec to report back network-based events that depart from accepted business use.

"We're monitoring segments of a corporation's internal network for appropriate use," Elgamal says.

By consulting with a company to understand how employees and business partners allowed inside the intranet use the network on a daily basis, Securify determines the security policy for appropriate use. "Then we can filter the data based on violations, and we'll generate alerts for critical violations based on the corporate policy," Elgamal says.

The Mountain View, Calif., company claims to have five customers for its service, which starts at $100,000 per year. Security installs its monitoring gear on the customer network.

The equipment reports policy violations back to Securify via servers stored at Exodus Communications.

"We've already found one customer had an employee running a separate Web server for his own business, with traffic inappropriately coming into the network for that," Elgamal says.

"There's no attack going on there, but there was inappriate access through the firewall that had nothing to do with the business of the company,"he adds.

Another security firm, RipTech, introduced its managed security service, dubbed Caltarian (Welsh for "wise shield," according to RipTech CTO Tim Belcher). At a starting price of $2,000 per device, per month, RipTech installs and remotely monitors any of six types of firewalls, intrusion-detection systems and VPNs from its Alexandria, Va., data center.

"We're offering real-time security monitoring for commercial organizations," Belcher says.

The Washington Times and United Press International, both owned by the same parent company, have signed up for the RipTech firewall service. Management earlier balked at the cost of buying a firewall, says Eric Johnson, Webmaster for The Washington Times.

But the managed firewall service from RipTech, which recommended the Cisco PIX, was viewed as more costeffective than buying one."It's $43,000 per year but we couldn't have hired a security specialist to handle this round-the-clock at that price," Johnson says.

RipTech and Securify compete against Counterpane and Internet Security Systems, among others, in the area of managed security services.

Cisco wants to make sure its equipment is widely used by providers. Toward that end, it has announced a vendor qualification program to certify service providers using the Cisco firewall, IDS and VPN to remotely manage services for their customers.

Exodus is the first certified provider, says Dan Hession, Cisco's director of service provider marketing for the VPN and security business unit. Cisco plans to recommend to its customers the service providers certified under the program and co-market managed security services with them.

Securify: www.securify.com; RipTech: www.riptech.com; Cisco: www.cisco.com

Taher Elgamal, CEO, Securify

Tim Belcher, CTO, RipTech